

REMARKS**1.) Claim Rejections – 35 U.S.C. § 103**

Claims 1-41 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,237,610 issued to Gammie et al. (hereinafter "Gammie"). Before addressing this rejection in detail, it should be noted that the Examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. *MPEP 2142*. To establish *prima facie* case of obviousness, certain criteria must be met. *First*, the prior art reference or references when combined must teach or suggest all the claim limitations. *Second*, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. With the above requirements in mind, Applicants respectfully traverse this rejection per discussion below.

Regarding independent claim 1, it is directed to a decryption system that comprises [1] a decryption unit, [2] a receiver for receiving encrypted data defining a *program decryption key* (a first key) and [3] a security processor being configured to decrypt the encrypted data using a program key (a second key) **so as to extract the first key from such encrypted data** and to output the program decryption key to the decryption unit that would use such key to decrypt encrypted program signals. See, e.g., *Figure 4*. Applicants respectfully submit the Gammie, as relied on by the Examiner, fails to teach or suggest at least one limitation as specified in claim 1.

Turning to Gammie, the Examiner relies on it to disclose all of the limitations of claim 1 *except* for the claimed interface, which the Examiner alleges to be well known in the art. *Office Action, pages 2-3*. With respect to Gammie, the Examiner relies on its *Figure 7* to teach or suggest many limitations as specified in claim 1. *Figure 7* discloses an encoder 701 and a decoder 706. The encoder 701 scrambles a source program 702 with a key from a key memory 704 and then the **key itself is twice-encrypted** by first and second key encryptors 710 and 715 and multiplexed with the scrambled program source for transmission to the decoder 706. *Abstract, Figure 7 and column 11, lines 59-65*. Regarding the encryption of such key, the first key encryptor 710 encrypts the key

Page 12 of 15

by using a first secret serial number such as SSN_0 from a first database 711 and then the second key encryptor 715 encrypts the partially encrypted key with a second secret serial number such as SSN_1 from a second database 716. *Abstract, Figure 7 and column 12, lines 5-19.*

To decode the encoded signal received from the encoder 701 via a transmission link 705, the decoder 706 performs a first key decryption, e.g., by using the secret serial number SSN_0 , which is also stored within a memory 712 and thus **already known** by the decoder 706. *Abstract, Figure 7 and column 12, lines 20-30.* The **partially decrypted key is then further decrypted** by a replaceable security module 714, e.g., by using the secret serial number SSN_1 , which is also stored within a memory 717 and thus **already known** by the replaceable security module 714. *Abstract, Figure 7 and column 12, lines 20-30.* The replaceable security module 714 is mounted on the exterior of the decoder. The decoder 706 then descrambles the source program using the twice-decrypted key.

Based on the above discussion of Gammie, Applicants respectfully submit that Gammie fails to teach or suggest at least one limitation such as the security processor of the claimed decrypting system, which **extracts** the program decryption key from the received encrypted data. Once extracted, the security processor outputs the program decryption key to the decryption unit of the decrypting system and such decryption system that would use such key to decrypt encrypted program signals. Regarding Gammie, its decoder 706 uses secret serial numbers to decrypt the received, encoded signal. Since such secret serial numbers are **already known** before decoding begins, the decoder 706 just uses them for decoding and thus there is **no need** for Gammie to **extract** any information such as a key from the received, encoded signal.

More specifically, assuming *arguendo* that the replaceable external security module 714 of Gammie is similar to the claimed security processor and that the fixed internal security module is similar to the claimed decryption unit, the replaceable external security module 714 would decrypt encoded data by using the secret serial number being stored in its memory 717 so as to yield a partially decrypted key and the fixed internal security module 719 would thereafter decrypt the partially decrypted key by using its own secret serial number being stored in its memory 712. In other words,

Page 13 of 15

the fixed internal security module 719 **does not require a key from another source** to perform its decryption since it already has and knows the secret serial number. In contrast, the claimed decryption unit (being similar to the fixed internal security module 719) **uses a program decryption key** to decrypt encrypted program signals and such program decryption key is **provided to the decryption unit from the claimed security processor** (being similar to the replaceable external security module 714 per assumption) after the extraction of such program decryption key from encrypted data by the security processor.

With respect to the Examiner's allegation that the interface as specified in claim 1 is well known, Applicants respectfully disagree and request the Examiner to provide a prior reference to support the Examiner's current allegation.

In addition, Applicants respectfully request the Examiner to **clearly** provide some suggestion or motivation why Gammie and the allegedly well known interface should or could be combined so as to yield the decryption system of claim 1.

Furthermore, even assuming *arguendo* that there is motivation or suggestion to combine Gammie and the allegedly well known interface, their combination would still fail to teach or suggest the decrypting system of claim 1 since Gammie fails to teach or suggest certain limitations of claim 1 as discussed above.

Based on the above discussion, Gammie fails to teach or suggest at least one limitation of claim 1 and accordingly, claim 1 is believed to be non-obvious and patentably distinguishable over Gammie.

Regarding claims 2-11, they depend from independent claim 1, which is believed to be patentable, and thus they should also be non-obvious and patentably distinguishable. *MPEP 2143.03*.

Regarding independent claim 12, it contains at least one limitation that is similar to at least one limitation of claim 1, which is believed to be patentable. Accordingly, claim 12 should be non-obvious and patentably distinguishable over Gammie for reasons similar to those discussed above regarding claim 1.

Page 14 of 15

Regarding claims 13-20, they depend from independent claim 12, which is believed to be patentable, and thus they should also be non-obvious and patentably distinguishable. *MPEP 2143.03*.

Regarding independent claim 21, it contains at least one limitation that is similar to at least one limitation of claim 1, which is believed to be patentable. Accordingly, claim 21 should be non-obvious and patentably distinguishable over Gammie for reasons similar to those discussed above regarding claim 1.

Regarding independent claim 22, it contains at least one limitation that is similar to at least one limitation of claim 1, which is believed to be patentable. Accordingly, claim 22 should be non-obvious and patentably distinguishable over Gammie for reasons similar to those discussed above regarding claim 1.

Regarding independent claim 23, it contains at least one limitation that is similar to at least one limitation of claim 1, which is believed to be patentable. Accordingly, claim 23 should be non-obvious and patentably distinguishable over Gammie for reasons similar to those discussed above regarding claim 1.

Regarding claims 24-32, they depend from independent claim 23, which is believed to be patentable, and thus they should also be non-obvious and patentably distinguishable. *MPEP 2143.03*.

Regarding independent claim 33, it contains at least one limitation that is similar to at least one limitation of claim 1, which is believed to be patentable. Accordingly, claim 33 should be non-obvious and patentably distinguishable over Gammie for reasons similar to those discussed above regarding claim 1.

Regarding claims 34-41, they depend from independent claim 33, which is believed to be patentable, and thus they should also be non-obvious and patentably distinguishable. *MPEP 2143.03*.

Page 15 of 15

CONCLUSION

Claims 1-41 are presently standing in this patent application. In view of the foregoing remarks, each and every point raised in the Office Action mailed on October 6, 2005 has been addressed on the basis of the above remarks. Applicants believe all of the claims currently pending in this patent application to be in a condition for allowance. Reconsideration and withdrawal of the rejections are respectfully requested. However, should the Examiner believe that direct contact with Applicants' attorney would advance the prosecution of the application, the Examiner is invited to telephone the undersigned at the number given below.

Respectfully submitted,



by Dang M. Vo
Registration No. 45,183

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502